СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Межсетевое экранирование

СПбГЭТУ «ЛЭТИ», 2021 г.

5. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ. НАСТРОЙКА ACLСПИСКОВ НА МАРШРУТИЗАТОРЕ CISCO

Цель работы: изучение теоретического материала о фильтрации сетевого трафика, формирование практических навыков построения список доступа и настройка NAT на межсетевом экране Cisco.

5.1. Межсетевое экранирование

Основой обеспечения защиты периметра выступает межсетевой экран. Межсетевой экран (МЭ) – аппаратный, программно-аппаратный или программный комплекс, реализующий функции управления, контроля и фильтрации сетевых информационных потоков между двумя и более ЛВС по некоторому набору правил, определяемых политикой безопасности.

МЭ как средство обеспечения безопасности, реализует следующие механизмы защиты:

-фильтрация трафика и ревизия содержимого пакетов (осуществляется на интерфейсе с использованием пакетной фильтрации и определением какой трафик обрабатывать приоритетнее);

-управление списками доступа на межсетевых экранах (путем ограничения доступа к маршрутизатору);

-использование технологий виртуальных частных сетей VPN (определением какой трафик нужно шифровать и какими криптоалгоритмами);

трансляция адресов (NAT- какие адреса необходимо транслировать);

-идентификация и аутентификация пользователей стандартных служб;

-противодействие некоторым видам атак на внутренние ресурсы.

Фильтрация трафика осуществляется на основании списков доступа -ACL (Access Control List) —набор текстовых выражений, которые определяют, на основании каких характеристик пакет может перейти через границы шлюза. Основное применение списков доступа пакетная фильтрация, при которой ACL не только разрешают или запрещают прохождения пакетов из внешней во внутреннюю сеть, но также могут просматривать тип пакета и порты назначения.

Изначально листы ACL формируются системным администратором, а затем размещаются на интерфейсах, для последующей фильтрации. Маршрутизатор/межсетевой экран рассматривает трафик как входящий и исходящий. Соответственно для каждого вида трафика ACL размещаются на входящем или на исходящем направлении интерфейса.

При получении пакета из сети МСЭ: проверяет имеется ли ACL на интерфейсе, в случае наличия дальнейшая обработка ведется по правилам списка доступа строго в том порядке, в котором записаны выражения. Если правила фильтрации позволяют прохождение пакета, то он отправляется на соответствующий интерфейс, в противном случае, пакет уничтожается.

Сам же ACL представляет собой последовательный набор текстовых выражений, в которых указаны характеристики пакета (IP, порт, протокол и др) и действия, которые необходимо выполнить над пакетом: permit (разрешить прохождение), deny (запретить прохождение пакета), обработка ведется строго в том порядке, в котором заданы выражения. ACL разделяются на два типа:

- *Стандартные* (Standard)-осуществляют только проверку адреса источника. Формат синтаксиса команд стандартного списка ACL [1]:

access-list access-list-number {permit|deny}
{host|source source-wildcard|any}

Пример использования стандартного списка ACL для блокирования всего трафика за исключением трафика из источника 10.1.1.x [1].

interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
access-list 1 permit 10.1.1.0 0.0.0.255

- *Расширенные* (Extended): осуществляют проверку адреса источник, тип протокола и адресованный порт, однако имею более низкую производительность.

Ниже приведен формат синтаксиса команд расширенных списков ACL для различных протоколов:

IP

access-list access-list-number [dynamic dynamic-name [timeout minutes]]

{deny | permit} protocol source source-wildcard
destination destination-wildcard [precedence precedence]
[tos tos] [log | log-input] [time-range time-range-name]

ICMP

access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard
destination destination-wildcard
[icmp-type | [[icmp-type icmp-code] | [icmp-message]]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name]

TCP

access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]] [established]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name]

UDP

access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name]

При создании ACL каждая запись списка доступа обозначается порядковым номером, по умолчанию в рамках десяти (10, 20, 30 и т.д) это позволяет системному администратору корректировать списки доступа не удаляя их, но необходимо учитывать, что ACL не действует на трафик, сгенерированный самим маршрутизатором. Расширенные ACL нужно размещать как можно ближе к источнику, стандартные же как можно ближе к получателю. Это нужно для того, чтобы не гонять пакеты по всей сети зря.

Подробнее о списках контроля доступа, а также об их синтаксисе в оборудовании компании Cisco можно прочитать в [1].

5.2. Задание

Разработать правила фильтрации с номерами для рабочих станций, коммутаторов и маршрутизаторов в соответствии со схемой, представленной в практической работе 1, настроить правила управления доступом к серверам и рабочим станциям из ЛВС в сеть Интернет и из нее к серверам, расположенным в ЛВС. Доступ в сеть Интернет из сети осуществляет по технологии NAT.

5.3. Порядок выполнения работы

5.3.1. Настройка ACLсписков на маршрутизаторе

На основании спроектированной в лабораторной работе 1 сетевой инфраструктуре осуществить настройку списков доступа Access-List на router2 и router3, для ограничения доступа злоумышленников к внутренней сети (Рис. 5.1).

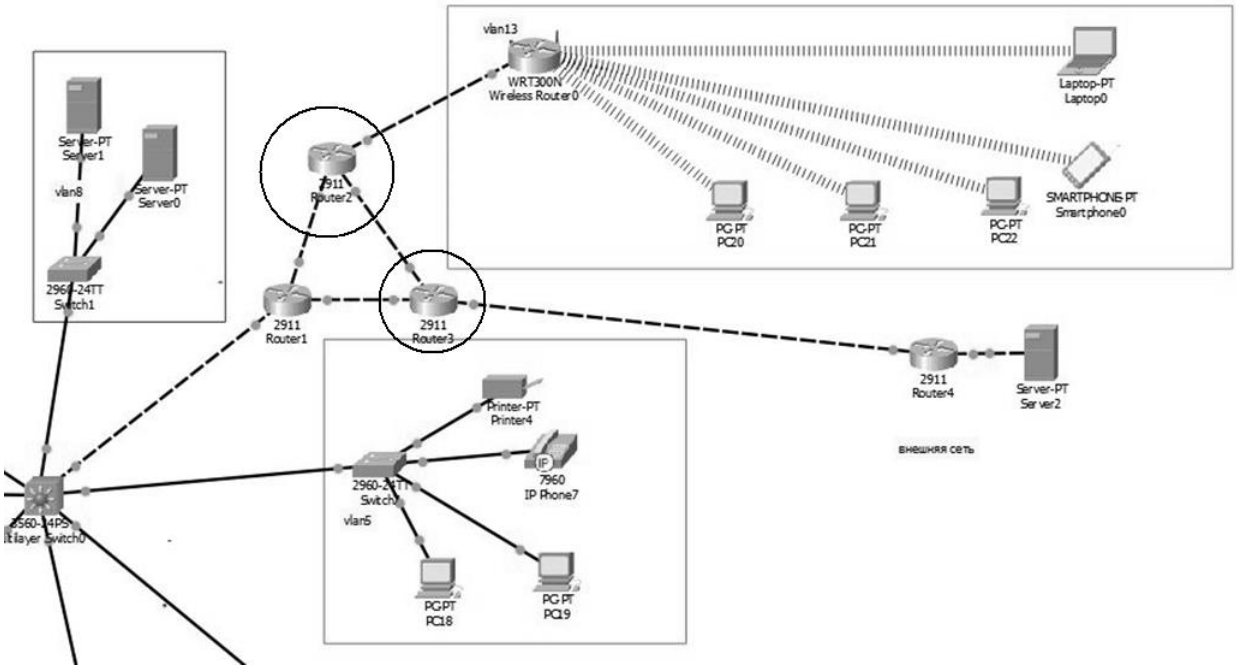

Рис. 5.1

Для этого в качестве примера разграничим доступ к внутренней сети на входе, для того чтобы уменьшить трафик, проходящий в маршрутизаторе и увеличить производительность внутренней ЛВС. Для этого необходимо ограничить трафик по разным характеристикам (используемые протоколы,

порты назначения, IP адреса) поэтому целесообразно использовать расширенные списки доступа. При формировании периметра защиты необходимо рассмотреть формирование различных ДМЗ, в частности можно выделить зоны, защищающие серверную часть (router3) и осуществить настройку списков доступа для трафика проходящего через router2 для ограничения доступа к ЛВС через Wi-Fi.

1. Сформировать расширенный список доступа для router2 согласно представленным командам:

   Conf t
   ip access-list extended for-out
   deny ip any 192.168.2.0 0.0.0.255 any eq 80
   deny ip any 192.168.3.0 0.0.0.255 eq 53
   deny ip any 192.168.4.0 0.0.0.255 eq 53
   deny ip any 192.168.5.0 0.0.0.255
   deny ip any 192.168.6.0 0.0.0.255
   deny ip any 192.168.7.0 0.0.0.255
   permit tcp host 10.194.210.11 host 192.168.7.0 0.0.0.255 eq 53
   permit ip any an
   exit

2. Прикрепить сформированный список доступа к интерфейсу маршрутризатора router2 для фильтрации на входящий трафик:

   Int gig0/2
   ip access-group for-out in
   end
   wr mem

3. Для проверки работы списка доступа проверить соединение эхо-пакетами через команду ping с узла подключённого по Wi-fi на узел находящийся внутри рабочей локальной сети (Рис. 5.2).

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рис. 5.2

4. Осуществить настройку Access-List на router3 с использованием следующих команд:

   En

   Conf t

   ip access-list extended from-out

   permit ip any 192.168.9.0 0.0.0.255

   permit ip any host 213.234.10.2

   exit

5. Прикрепить сформированный список доступа к интерфейсу маршрутризатора router3:

   Int gig0/1

   ip access-group from-out in

   end

   wr mem

6. Для проверки работы списка доступа сформировать соединение эхо-пакетами через команду ping с узла локальной сети, эхо-пакет не должен проходить (Рис. 5.3 и 5.4).

```
Pinging 213.234.10.2 with 32 bytes of data:

Reply from 213.234.10.2: bytes=32 time=2ms TTL=254
Reply from 213.234.10.2: bytes=32 time=24ms TTL=254
Reply from 213.234.10.2: bytes=32 time=16ms TTL=254
Reply from 213.234.10.2: bytes=32 time<1ms TTL=254

Ping statistics for 213.234.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 24ms, Average = 10ms

C:\>ping 213.234.10.2

Pinging 213.234.10.2 with 32 bytes of data:

Reply from 213.234.10.2: bytes=32 time=10ms TTL=254
Reply from 213.234.10.2: bytes=32 time<1ms TTL=254
Reply from 213.234.10.2: bytes=32 time=25ms TTL=254
Reply from 213.234.10.2: bytes=32 time<1ms TTL=254

Ping statistics for 213.234.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 25ms, Average = 8ms
```

Рис. 5.3

```
Router>en
Router#ping 192.168.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2
seconds:
.UUUU
Success rate is 0 percent (0/5)

Router#ping 192.168.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2
seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Рис. 5.4

Примечание: При редактировании ACL записи вставляются в порядке ввода. Нельзя вставить новую запись между двумя уже введенными. Если это все-таки надо сделать, то необходимо:

- скопировать все правила из конфигурации в блокнот;
- вставить необходимые записи;
- удалить весь список;
- скопировать все записи из блокнота и прикрепить к интерфейсу.

5.3.2 Настройка NAT на межсетевом экране

Технология NAT применяется как для обеспечения доступа узлов с немаршрутизируемыми адресами к сети Интернет, так и для реализации механизмов защиты сети, например, для изоляции сетей управления или прохождения пакетов через VPN-шлюз.

Существуют следующие виды NAT: динамическая трансляция адресов на уровне портов, динамическая трансляция на уровне портов с выборкой IP-адресов, трансляция с динамической выборкой IP-адресов и статическая трансляция. Согласно нашей имеющейся схеме (Рис. 5.1) выполним в качестве примера настройку на router 3. По схеме за ним следует роутер и сервер с белыми адресами, так же на router 3 прописан белый адрес 213.234.10.2 на порте, соединенном с провайдером.

1. Прописать шлюз на роутере с IP адресом 213.234.10.1 (Рис. 5.5)

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 213.234.10.1
Router(config)#do wr mem
Building configuration...
[OK]
Router(config)#
```

Рис. 5.5

2. Проверить интерфейсы и явно указать, какие из них являются внешними, а какие внутренними (Рис. 5.6, 192.168.0.0)

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip nat ou
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int gig0/0
Router(config-if)#ip nat ins
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int gig0/2
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#do wr mem
Building configuration...
[OK]
Router(config)#
```

Рис. 5.6

3. Настроить списки доступа к внешней сети из диапазона 192.168.2.0-192.168.9.0 и включить службу NAT (Рис 5.7).

```
Router(config)#ip access-list stan
Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.3.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.4.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.8.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.9.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.5.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.6.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.7.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#ip nat ?
  inside   Inside address translation
  outside  Outside address translation
  pool     Define pool of addresses
Router(config)#ip nat ins
Router(config)#ip nat inside ?
  source  Source address translation
Router(config)#ip nat inside sour
Router(config)#ip nat inside source ?
  list    Specify access list describing local addresses
  static  Specify static local->global mapping
Router(config)#ip nat inside source FOR-NAT ?
% Unrecognized command
Router(config)#ip nat inside source list FOR-NAT  ?
  interface  Specify interface for global address
  pool       Name pool of global addresses
Router(config)#ip nat inside source list FOR-NAT  int
Router(config)#ip nat inside source list FOR-NAT  interface gig0/1
Router(config)#do wr mem
Building configuration...
[OK]
Router(config)#ip nat inside source list FOR-NAT  interface gig0/1 overlo
Router(config)#ip nat inside source list FOR-NAT  interface gig0/1 overload
Router(config)#do wr mem
Building configuration...
[OK]
Router(config)#
```

Рис. 5.7

4. Проверить корректность функционирования оборудования, возможность доступа из внешней сети к общедоступным сервисам и из корпоративной ЛВС. Рассмотреть необходимость использования статической маршрутизации.
5. *Дополнительное задание*: Используя [3, стр 76-80] создать и настроить политику безопасности протокола ISAKMP со следующими параметрами: метод аутентификации – PSK, алгоритм шифрования – AES, алгоритм хэширования – SHA1, номер группы Диффи-Хеллмана – 5, длина вырабатываемого ключа – 1 536 бит.

6. Разработать политику безопасности, сформировать ДМЗ, а также фильтрации с номерами для рабочих станций, коммутаторов и маршрутизаторов в соответствии со схемой, представленной в практической работе 1.
7. Настроить правила управления доступом к серверам и рабочим станциям из ЛВС в сеть Интернет и из нее к серверам, расположенным в ЛВС. Доступ в сеть Интернет из сети осуществляет по технологии NAT.

3.4. Контрольные вопросы

1. Какой диапазон номеров выделен для расширенных списков доступа IP?
2. Списки доступа какого типа позволяют блокировать отдельные порты?
3. Как конфигурируется NAT: глобально или для отдельного интерфейса?
4. Сконфигурируйте расширенный список доступа, блокирующий входящий трафик HTTP.
5. Сконфигурируйте на маршрутизаторе NAT для внутренней сети 192.168.3.23 и внешнего интернет соединения с адресом 115.68.43.1. Внутренний интерфейс – ethernet 0, внешний – serial 0; адрес внутреннего интерфейса – 192.168.3.1.

СПИСОК ЛИТЕРАТУРЫ

1. Настройка списков доступа IP. Электронный ресурс https://www.cisco.com/c/ru_ru/support/docs/security/ios-firewall/23602-confaccesslists.html#acltypes.
2. Интуит. Лекция 9: Списки доступа ACL. Настройка статического и динамического NAT. Электронный ресурс https://intuit.ru/studies/courses/3549/791/lecture/29226?page=1.
3. Д.Н. Колегов. Лабораторный практикум по построению компьютерных сетей. Лабораторный практикум по основам построения защищенных

компьютерных сетей. Томск: Томский государственный университет, 2013. – 140 с

4. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. – Пер. с англ. – СПб: СимволПлюс, 2003. – 512 с., ил